PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-214482

(43)Date of publication of application : 15.08.1997

(51)Int.Cl. H04L 9/30
G09C 1/00

(21)Application number : 08-016707

(22)Date of filing : 01.02.1996

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

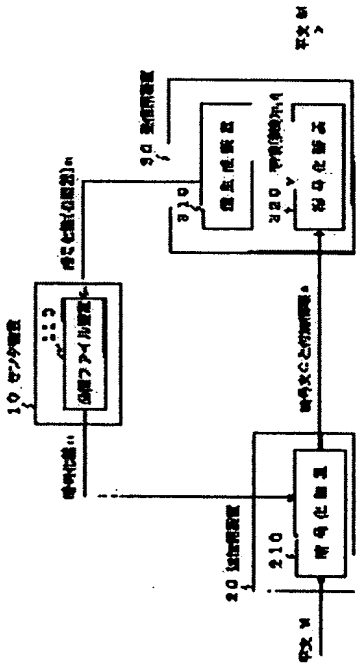
(72)Inventor : KUWAKADO SHUSUKE
KOYAMA KENJI

(54) PUBLIC KEY CIPHERING METHOD AND PUBLIC KEY CIPHERING COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To make difficulty of decoding equivalent to difficulty of factorization into prime factors, to attain definite decoding with additional information of a simple calculation and to attain high speed decoding.

SOLUTION: A key generator 310 generates two primes p, q, to obtain n=pq, and a value (n) is registered in a public file device 110 as a ciphering key and the values p, q are stored in a decoder 320 as decoding keys. A ciphering device 210 uses the ciphering key (n) and a plain text M, a point C=(cx, cy) obtained doubling the plain text N=(mx, my) on an ellipse by2=x3+x(mad n) is used for a ciphered text and additional information (e) and the ciphered text are sent. A decoder 320 uses decoding keys p, q to apply a multiple of 1/2 to the ciphered text C on the ellipse by2=x3+x (mod p, q) to obtain objects M1(i=1-4). In this case, a formula of a solution of a quartic equation is used. The plain text M is selected by using the additional information (e) from the objects M1.



LEGAL STATUS

[Date of request for examination]	01.02.1996
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2836059
[Date of registration]	09.10.1998
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－214482

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/30			Ｈ０４Ｌ	9/00	６６３Ａ
Ｇ０９Ｃ	1/00	６２０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６２０Ａ

審査請求　有　　請求項の数２　ＯＬ　（全９頁）

(21)出願番号　特願平8－16707

(22)出願日　平成８年(1996)２月１日

特許法第30条第１項適用申請有り　1995年12月14日　社団法人電子情報通信学会開催の「情報セキュリティ研究会」において文書をもって発表

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　桑門　秀典
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　小山　謙二
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

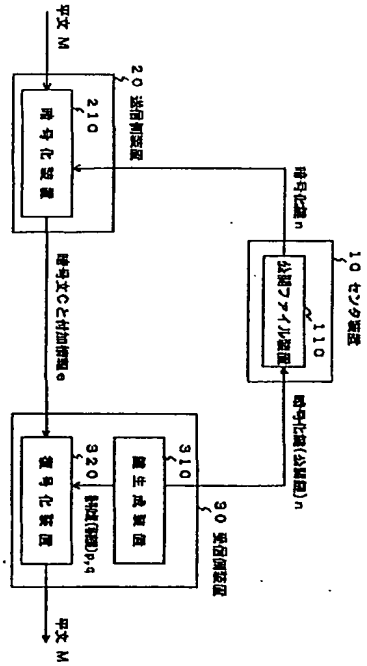
(74)代理人　弁理士　鈴木　誠

(54)【発明の名称】　公開鍵暗号方法及び公開鍵暗号通信システム

(57)【要約】

【課題】　解読の難しさが素因数分解の難しさと等価であり、かつ簡単な計算の付加情報で一意の復号を可能とし、さらに高速な復号化を可能とする。

【解決手段】　鍵生成装置３１０は、２つの素数ｐ，ｑを生成し、ｎ＝ｐｑを求め、ｎを暗号化鍵として公開ファイル装置１１０に登録し、ｐとｑを復号化鍵として復号化装置３２０で記憶する。暗号化装置２１０は、暗号化鍵ｎと平文Ｍにより、平文Ｍ＝（m_x，m_y）を楕円曲線$by^2 \equiv x^3 + x \pmod n$上で２倍した点Ｃ＝（$c_x$，$c_y$）を暗号文とし、付加情報ｅをともに送出する。復号化装置３２０は、復号化鍵ｐ，ｑにより、暗号文Ｃを楕円曲線$by^2 \equiv x^3 + x \pmod{p, q}$上で１／２倍し、候補$M_i$（ｉ＝１～４）を求める。その際、４次方程式の解の公式を用いる。候補M_iより付加情報ｅを用いて平文Ｍを選ぶ。



1

【特許請求の範囲】

【請求項１】　楕円曲線上の演算を利用した一意復号可能な公開鍵暗号方法であって、

２つの素数ｐ，ｑを生成し、ｎ＝ｐｑを計算し、ｎを公開鍵の暗号化鍵、ｐとｑを秘密鍵の復号化鍵とし、

暗号化鍵ｎと平文Ｍ＝（m_x，m_y）から、平文Ｍ＝（m_x，m_y）を楕円曲線ｂ$y^2 \equiv x^3 + x$（mod ｎ）上で２倍した点Ｃ＝（c_x，c_y）を計算して、前記Ｃ＝（c_x，c_y）を暗号文とし、かつ、一意復号のための付加情報ｅを求め、

復号化鍵ｐ，ｑと暗号文Ｃから、４次方程式の解の公式を用いて、暗号文Ｃ＝（c_x，c_y）を楕円曲線ｂ$y^2 \equiv x^3 + x$（mod ｐ，ｑ）上で１／２倍して、平文の候補M_i（ｉ＝１～４）を求め、付加情報ｅにより、候補M_i（ｉ＝１～４）の中から平文Ｍを決定することを特徴とする公開鍵暗号方法。

【請求項２】　鍵生成装置、暗号化装置、復号化装置、公開ファイル装置、及び、これら装置を結ぶ通信路から構成され、楕円曲線上の演算を利用した一意復号可能な公開鍵暗号通信システムであって、

前記鍵生成装置は、２つの素数ｐ，ｑを生成し、該ｐ，ｑを秘密鍵の復号化鍵として前記復号化装置に記憶する手段と、前記生成した素数ｐ，ｑの積ｎ（ｎ＝ｐｑ）を計算し、該ｎを公開鍵の暗号化鍵として前記公開ファイル装置へ登録する手段とを有し、

前記暗号化装置は、前記公開ファイル装置から暗号化鍵ｎを入手し、平文Ｍ＝（m_x，m_y）を楕円曲線ｂ$y^2 \equiv x^3 + x$（mod ｎ）上で２倍した点Ｃ＝（c_x，c_y）を計算し、暗号文Ｃとして前記復号化装置に送信する手段と、前記暗号化鍵ｎと平文Ｍ＝（m_x，m_y）から、ヤコビ記号（m_y／ｎ）の値e_1と、m_xと１／m_x mod ｎの大小関係を表わす値e_2とを求め、一意復号のための付加情報ｅ（＝e_1，e_2）として前記復号化装置に送信する手段とを有し、

前記復号化装置は、前記復号化鍵ｐ，ｑと暗号文Ｃから、４次方程式の解の公式を用いて、暗号文Ｃ＝（c_x，c_y）を楕円曲線ｂ$y^2 \equiv x^3 + x$（mod ｐ，ｑ）上で１／２倍して、平文の候補M_i＝（m_{x_i}，m_{y_i}）（ｉ＝１～４）を求める手段と、前記候補M_iの中から（m_{y_i}／ｎ）が前記付加情報e_1と同じM_i（ｊ＝１，２）を選び、該M_iから前記付加情報e_2により平文Ｍを決定する手段とを有する、ことを特徴とする公開鍵暗号通信システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ディジタル化された情報を伝送する際の暗号方法及び暗号通信システムに関し、詳しくは、楕円曲線上の演算を利用した一意復号可能な公開鍵暗号方法及び公開鍵暗号通信システムに関する。

2

【０００２】

【従来の技術】従来の楕円曲線上の演算を暗号化復号化に利用した公開鍵暗号方式としては、楕円曲線$y^2 \equiv x^3 + b$（mod ｎ）を利用した楕円ラビン方式が知られている例えば、K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone, ; "New public-key schemes based on elliptic curves over the ring Z_n", Advances in Cryptology－Crypto' ９１, ＬＮＣＳ ５７６, pp. ２５２－２６６, １９９１参照）。

【０００３】この楕円ラビン方式は、解読の難しさが素因数分解の難しさと等価であることが数学的に証明されている。しかし、楕円ラビン方式は、暗号化関数が多対一関数なので、暗号文を復号化すると、複数個の平文の候補が得られ、受信者にはどれが送信者の送りたい平文なのかわからなかった（復号の多義性）。また、楕円ラビン方式では、復号化にも楕円曲線上の演算を利用しているので、復号化速度が遅かった。

【０００４】

【発明が解決しようとする課題】従来の楕円ラビン方式は、上述の復号の多義性の問題であるので、何らかの付加情報により平文を決定する必要がある。しかしながら、安全性をそこなわずに平文を一意に決定するためには、どのような付加情報を送ればよいのかが不明であった。また、復号化速度が遅いことは実用化の際問題となる。

【０００５】本発明の目的は、従来の楕円ラビン方式と同様に解読の難しさが素因数分解の難しさと等価であり、かつ、簡単に計算できる付加情報により一意に復号が可能であり、かつ、復号化速度がより高速であるような楕円曲線上の演算を利用した公開鍵暗号方法及び公開鍵暗号通信システムを提供することにある。

【０００６】

【課題を解決するための手段】本発明の楕円曲線上の演算を利用した公開鍵暗号方方及び通信システムは、以下のことを特徴としている。

（１）　鍵生成では、２つの素数ｐ，ｑを生成し、ｎ＝ｐｑを計算し、ｎを暗号化鍵として公開し（公開鍵）、ｐとｑを復号化鍵として受信側が秘密に保持する（秘密鍵）。

（２）　送信側は、平文をＭ＝（m_x，m_y）とし、公開された受信者の暗号化鍵ｎと平文Ｍから、平文Ｍ＝（m_x，m_y）を楕円曲線ｂ$y^2 \equiv x^3 + x$（mod ｎ）上で２倍したＣ＝（c_x，c_y）を計算し、これを暗号文Ｃとして受信側に送信する。また、一意に復号するための情報として、簡単に計算できるヤコビ記号（m_y／ｎ）の値e_1と、m_xと１／m_x mod ｎ の大小関係を表わす値e_2とを、暗号文の付加情報として受信側に送信する。

（３）　受信側は、秘密の復号化鍵ｐ，ｑにより、暗号文Ｃ＝（c_x，c_y）を楕円曲線ｂ$y^2 \equiv x^3 + x$（mod ｐ，ｑ）上で１／２倍する。この１／２倍を計算する際、復

号化をより高速に行うために４次方程式の解の公式を用いる。暗号文Ｃを１／２倍した点は４つ存在するので、それらを平文の候補M_i（ｉ＝１～４）とおく。このM_i（ｉ＝１～４）の中から、付加情報e_1，e_2を用いて平文Ｍを選ぶ。

【０００７】

【発明の実施の形態】以下、本発明の一実施の形態について図面を用いて説明する。図１は、本発明の公開鍵暗号方式が適用される通信システムの全体ブロック図を示す。図１において、１０はセンタ装置、２０は送信側装置、３０は受信側装置である。センタ装置１０は、利用者から任意に参照可能な公開ファイル装置１１０を有している。送信側装置２０は暗号化装置２１０を有し、受信側装置３０は鍵生成装置３１０と復号化装置３２０を有する。

【０００８】あらかじめ鍵生成装置３１０にて、暗号化鍵ｎと復号化鍵ｐ、ｑを生成し、暗号化鍵ｎは公開鍵として公開ファイル装置１１０に登録し、復号化鍵ｐ、ｑは秘密鍵として復号化装置３２０に記憶しておく。センタ装置１０の公開ファイル装置１１０には、該鍵生成装置３１０によって生成された暗号化鍵ｎが、それぞれ利用者毎に登録されている。

【０００９】送信側装置２０では、公開ファイル装置１１０より相手受信者の暗号化鍵ｎを入手し、暗号化装置２１０にて、入力された平文Ｍを該暗号化鍵ｎにより暗号化し、さらに付加情報ｅ（＝e_1，e_2）を生成し、その暗号文Ｃと付加情報ｅを受信側装置３０に送信する。受信側装置３０の復号化装置３２０では、暗号文Ｃを復＊号化鍵ｐ、ｑと付加情報ｅとによって一意に復号し、平文Ｍを出力する。

【００１０】なお、鍵生成装置３１０は、必ずしも受信側装置３０に設ける必要はなく、例えばセンタ装置１０に設けてもよいが、この場合には、復号化装置３２０が保持する復号化鍵ｐ，ｑの秘密性が保証される必要がある。

【００１１】以下に、鍵生成装置３１０、暗号化装置２１０及び復号化装置３２０の構成例を詳述する。

【００１２】〈鍵生成装置〉図２は、本発明の一実施例の鍵生成装置３１０の構成図を示す。素数生成器３１１は２つの素数ｐ、ｑを生成し、乗算器３１２はｎ＝ｐｑを計算する。ここで、ｎは暗号化鍵（公開鍵）として公開ファイル装置１１０に登録され、ｐとｑは復号化鍵（秘密鍵）として復号化装置３２０に記憶される。

【００１３】〈暗号化装置〉図３は、本発明の一実施例の暗号化装置２１０の構成図を示す。暗号化装置２１０には、入力として、暗号化鍵ｎと平文Ｍ＝（m_x，m_y）が与えられる。但し、$0<m_x<n$かつ$0<m_y<n$かつｇｃｄ（$m_x m_y$，ｎ）＝１とする。

【００１４】楕円曲線２倍算器２１１は、暗号化鍵ｎと平文Ｍ＝（m_x，m_y）から、該平文Ｍ＝（m_x，m_y）を楕円曲線$by^2 \equiv x^3+x \pmod n$上で２倍した点Ｃ＝（$c_x$，$c_y$）を計算し、暗号文Ｃとする。具体的には、楕円曲線２倍算器２１１では、

【００１５】

【数１】

$$\begin{aligned} c_x &= \frac{(3m_x^2+1)^2}{(2bm_y)^2} \cdot b - 2m_x \bmod n, \\ &= \frac{(m_x^2-1)^2}{4m_x(m_x^2+1)} \bmod n, \\ c_y &= \frac{3m_x^2+1}{2bm_y} \cdot (m_x - x_3) - m_y \bmod n, \\ &= \frac{(m_x^2-1)((m_x^2-1)^2+8m_x^2)m_y}{2(2m_x(m_x^2+1))^2} \bmod n, \end{aligned} \qquad (1)$$

【００１６】の計算が行われる。ここで、ｂの計算は不要であるが、形式的には、ｂ＝（$m_x^3+m_x$）／m_y^2 ｍｏｄ ｎを意味する。

【００１７】付加情報生成器２１２は、暗号化鍵ｎと平※文Ｍ＝（m_x，m_y）から、付加情報ｅ＝（e_1，e_2）を計算する。具体的には、付加情報生成器２１２では、

【００１８】

【数２】

$$e_1 = \left(\frac{m_y}{n}\right), \quad e_2 = \begin{cases} 0, & m_x > (1/m_x \bmod n)\text{のとき}, \\ 1, & \text{上記以外のとき}, \end{cases} \qquad (2)$$

【００１９】の計算が行なわれている。但し、（　）はヤコビ（Ｊａｃｏｂｉ）記号である。

【００２０】暗号化装置２１０は、求った暗号文Ｃ＝（c_x，c_y）と付加情報ｅ＝（e_1，e_2）を受信側装置３０に送出して、動作を終了する。

【００２１】〈復号化装置〉図４は、本発明の一実施例の復号化装置の構成図を示す。鍵生成装置３１０で生成された素数ｐ、ｑは各々記憶部３２１と記憶部３２２に

5 6

記憶されている。

【００２２】楕円曲線１／２倍算器３２３は、楕円曲線 $by^2 \equiv x^3 + x \pmod p$ 上の暗号文 $C = (c_x, c_y)$ の２つの１／２倍点 $Mp_1 = (m_{xp1}, m_{yp1})$、$Mp_2 = (m_{xp2}, m_{yp2})$ を計算する（復号化）。この場合、よ＊り少ない演算量で復号化するために、式（１）をmod pに還元した４次方程式を直接解いて１／２点（半点）を計算する。式（１）をmod pに還元した式から、解くべき４次方程式は以下のようになる。

【００２３】

$$x^4 - 4c_{xp}x^3 - 2x^2 - 4c_{xp}x + 1 \equiv 0 \pmod p \qquad (3)$$

ここで、c_{xp}は既知数である。式（３）に４次方程式の解の公式を適用すると、解x_i（$i = 1 \sim 4$）は形式的に以下のようになる。※

※【００２４】

【数３】

$$\begin{aligned}
x_1 &= c_{xp} - \sqrt{c_{xp}^2 + 1} - \sqrt{2c_{xp}^2 - 2c_{xp}\sqrt{c_{xp}^2+1}} \bmod p \\
x_2 &= c_{xp} - \sqrt{c_{xp}^2 + 1} + \sqrt{2c_{xp}^2 - 2c_{xp}\sqrt{c_{xp}^2+1}} \bmod p \\
x_3 &= c_{xp} + \sqrt{c_{xp}^2 + 1} - \sqrt{2c_{xp}^2 + 2c_{xp}\sqrt{c_{xp}^2+1}} \bmod p \\
x_4 &= c_{xp} + \sqrt{c_{xp}^2 + 1} + \sqrt{2c_{xp}^2 + 2c_{xp}\sqrt{c_{xp}^2+1}} \bmod p
\end{aligned} \qquad (4)$$

【００２５】式（４）は少なくとも解m_{xp}と$1/m_{xp}$ mod pをもつので、x_i（$i = 1 \sim 4$）のうち２つはm_{xp}と$1/m_{xp}$ mod pである。m_{xp}と$1/m_{xp}$ mod p以外の解はmod pでは存在しないことを示す。

★【００２６】具体的に、楕円曲線１／２倍計算器３２３では、次の計算が行われる。

【００２７】

★【数４】

$$\begin{aligned}
c_{xp} &= c_x \bmod p, \\
c_{yp} &= c_y \bmod p, \\
m_{xp1} &= c_{xp} + k_p + \sqrt{2c_{xp}^2 + 2c_{xp}k_p} \bmod p, \\
m_{xp2} &= c_{xp} + k_p - \sqrt{2c_{xp}^2 + 2c_{xp}k_p} \bmod p, \\
m_{yp1} &= \frac{2(2m_{xp1}(m_{xp1}^2+1))^2 c_{yp}}{(m_{xp1}^2-1)((m_{xp1}^2-1)^2 + 8m_{xp1}^2)} \bmod p, \\
m_{yp2} &= \frac{2(2m_{xp2}(m_{xp2}^2+1))^2 c_{yp}}{(m_{xp2}^2-1)((m_{xp2}^2-1)^2 + 8m_{xp2}^2)} \bmod p,
\end{aligned} \qquad (5)$$

【００２８】ここで、k_pは式（６）をみたす値である。

【００２９】

☆【数５】

$$k_p^2 \equiv c_{xp}^2 + 1 \pmod p \text{ and } \left(\frac{2c_{xp}^2 + 2c_{xp}k_p}{p}\right) = 1 \qquad (6)$$

【００３０】同様に楕円曲線１／２倍算器３２４は、楕円曲線 $by^2 \equiv x^3 + x \pmod q$ 上の暗号文 $C = (c_x, c_y)$ の２つの１／２倍点 $M_{q1} = (m_{xq1}, m_{yq1})$、$M_{q2} = (m_{xq2}, m_{yq2})$ を計算する。

【００３１】中国人剰余定理計算器３２４は、p、qと◆M_{p1}、M_{p2}、M_{q1}、M_{q2}から平文の４つの候補$M_i = (m_{xi}, m_{yi})$（$i = 1 \sim 4$）を計算する。具体的には、中国人剰余定理計算器３２５では、

【００３２】

【数６】

$$\begin{aligned}
M_1 = (m_{x1}, m_{y1}) &= (\mathrm{CRT}(m_{xp1}, m_{xq1}), \mathrm{CRT}(m_{yp1}, m_{yq1})), \\
M_2 = (m_{x2}, m_{y2}) &= (\mathrm{CRT}(m_{xp1}, m_{xq2}), \mathrm{CRT}(m_{yp1}, m_{yq2})), \\
M_3 = (m_{x3}, m_{y3}) &= (\mathrm{CRT}(m_{xp2}, m_{xq1}), \mathrm{CRT}(m_{yp2}, m_{yq1})), \\
&= (1/m_{x2} \bmod n, -m_{y2}/m_{x2}^2 \bmod n), \\
M_4 = (m_{x4}, m_{y4}) &= (\mathrm{CRT}(m_{xp2}, m_{xq2}), \mathrm{CRT}(m_{yp2}, m_{yq2})), \\
&= (1/m_{x1} \bmod n, -m_{y1}/m_{x1}^2 \bmod n).
\end{aligned} \qquad (7)$$

【００３３】の計算が行なわれる。ここで、ＣＲＴ（t_p、t_q）はt_p、t_qに中国人剰余定理を適用することを

7　　8

意味し、具体的には、式（８）で表わされる。

【００３４】

＊【数７】

$$CRT(t_p, t_q) = t_p \cdot (1/q \bmod p) \cdot q + t_q \cdot (1/p \bmod q) \cdot p \mod pq \quad (8)$$

【００３５】比較器３２６では、e_1を用いて、M_i＝（m_{xi}，m_{yi}）（ｉ＝１～４）の中から（m_{yi}／ｐｑ）がe_1と同じ点を選ぶ。このようなM_iは必ず２つある。それらをM_1、M_3とおく。次に、比較器３２７において、e_2を用いて、M_1とM_3のうち、e_2＝０ならばｘ座標値が大きい方、さもなければｘ座標値が小さい方を平文Ｍとして出力する。

【００３６】

【発明の効果】上述のように、本発明の公開鍵暗号方法及び公開鍵暗号通信システムによれば、解読の難しさが素因数分解の難しさと等価であり、即ち、全面的に解読することは暗号化鍵ｎを素因数分解することと等価であり、かつ、簡単に計算できる付加情報により一意に復号が可能であり、さらに、復号に４次方程式の解の公式を利用することにより、復号化速度のより高速化が可能である。

【図面の簡単な説明】

【図１】本発明の一実施例のシステム全体図である。

【図２】鍵生成装置の一実施例の構成図である。

【図３】暗号化装置の一実施例の構成図である。

【図４】復号化装置の一実施例を構成図である。

【符号の説明】

１１０　公開ファイル装置

２１０　暗号化装置

２１１　楕円曲線２倍算器

２１２　付加情報生成器

３１０　鍵生成装置

３１１　素数生成器

３１２　乗算器

３２０　復号化装置

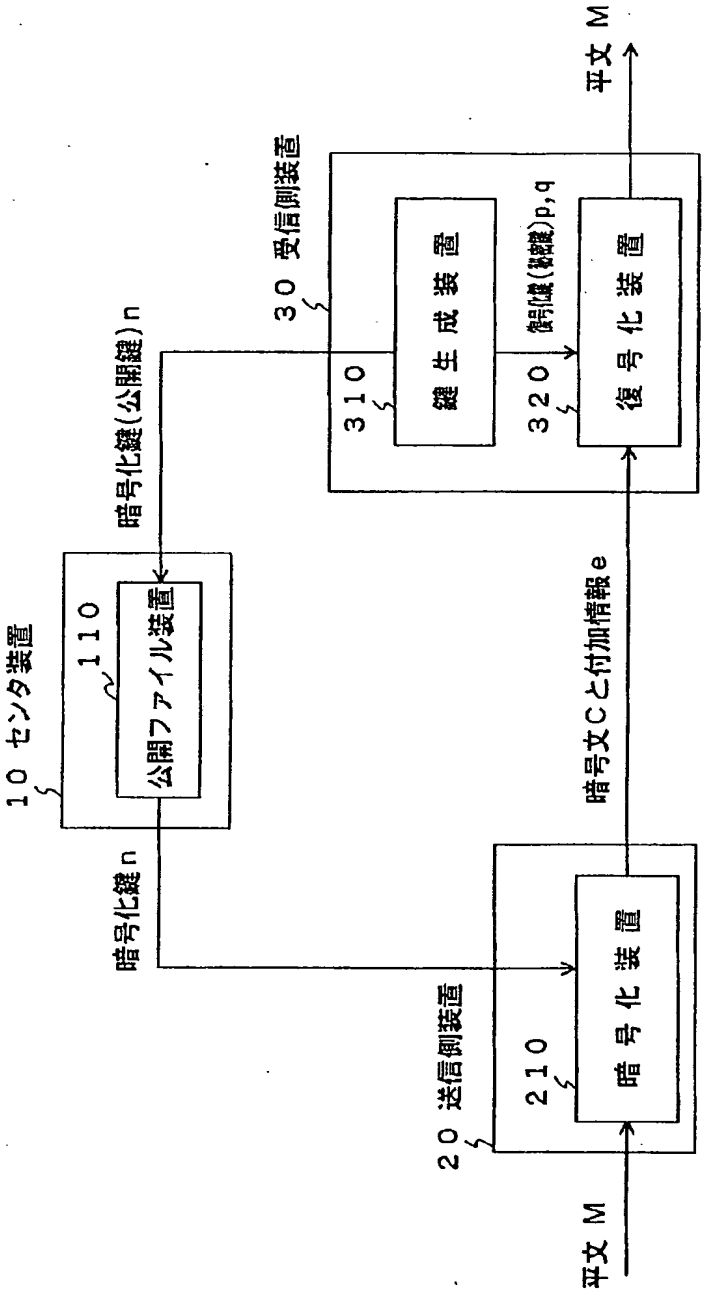
３２１，３２２　秘密鍵記憶部

３２３，３２４　楕円曲線１／２倍算器

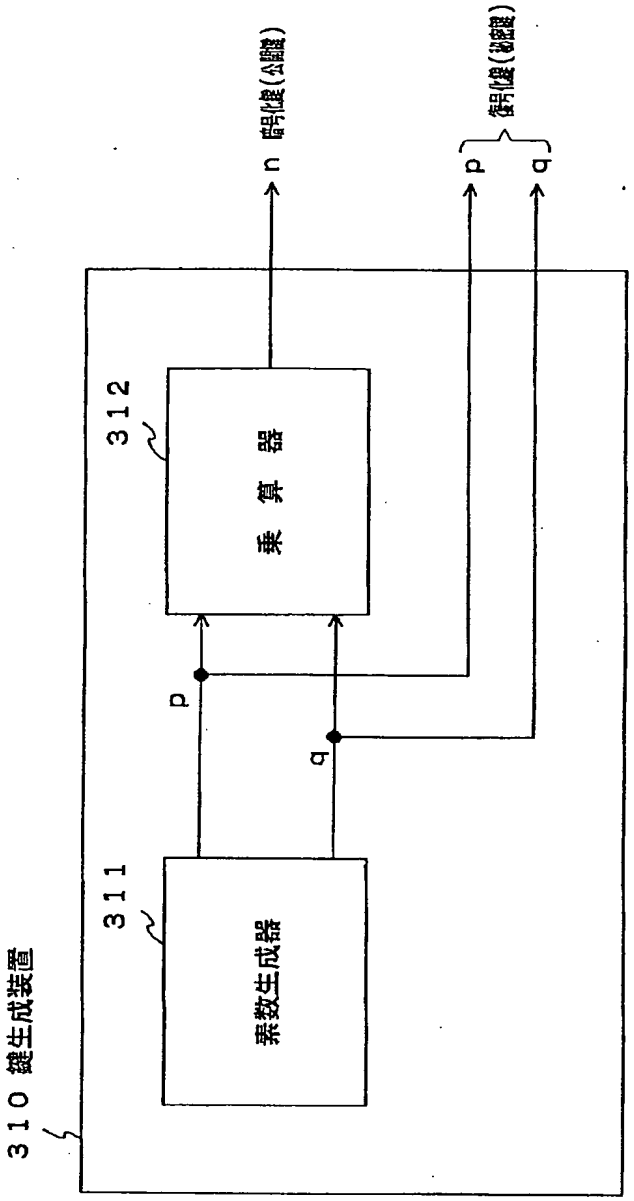
３２５　中国人剰余定理計算器

３２６，３２７　比較器

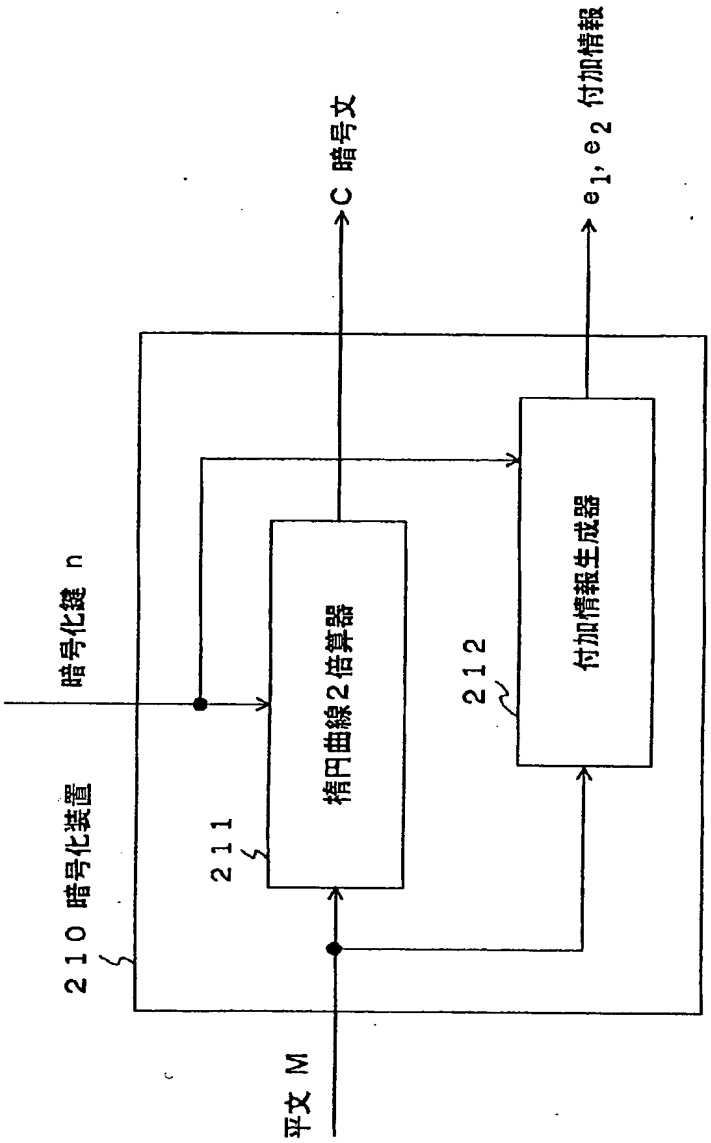
【図１】


１０ センタ装置
１１０
公開ファイル装置
暗号化鍵(公開鍵)ｎ
暗号化鍵ｎ
３０ 受信側装置
３１０
鍵生成装置
３２０
復号化装置
鍵(秘鍵)p,q
平文Ｍ
暗号文Ｃと付加情報ｅ
２０ 送信側装置
２１０
暗号化装置
平文Ｍ

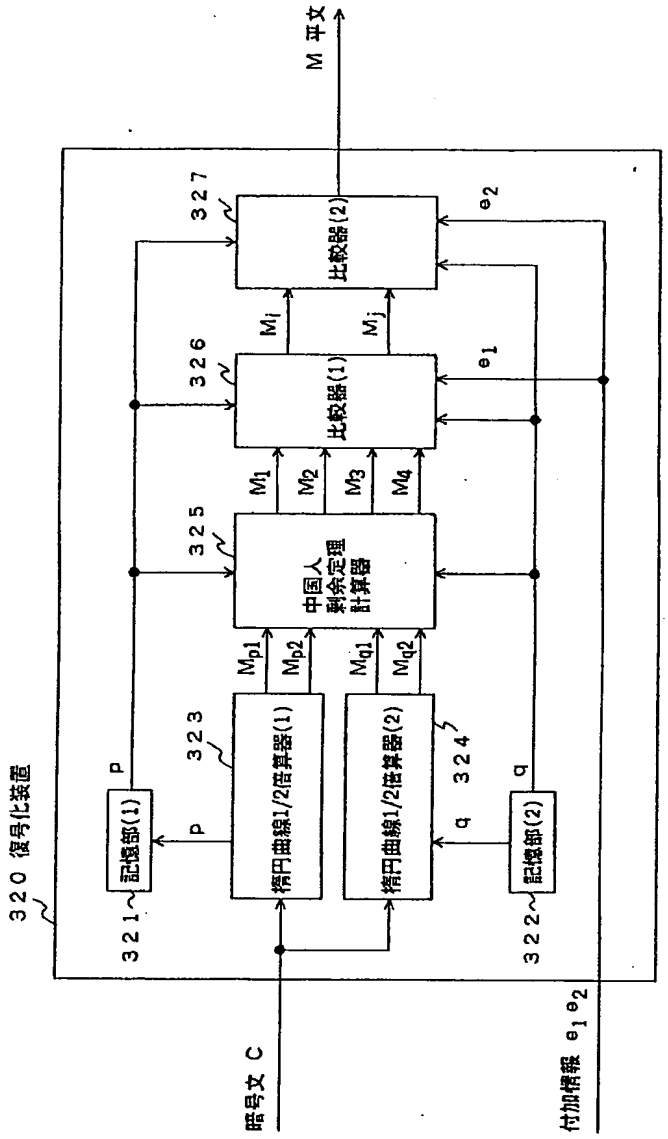
【図２】



【図３】



【図４】


M 平文
320 復号化装置
327
比較器(2)
326
比較器(1)
325
中国人剰余定理計算器
323
楕円曲線1/2倍算器(1)
324
楕円曲線1/2倍算器(2)
321
記憶部(1)
322
記憶部(2)
M1
M2
M3
M4
Mp1
Mp2
Mq1
Mq2
Mi
Mj
e1
e2
p
q
暗号文 C
付加情報 e1 e2